BA840 - Data Ethics - Team 2 Group Project
Christian Lawrence, Maraline Torres, Jiajian (Sylar) Guo, Jordan Grose, Antonio Moral

Introduction

Voice assistants and smart home devices have grown in popularity since Apple's initial release of "Siri" in 2011. Voice assistant capabilities have expanded far beyond a simple voice bot on a phone that can tell you the weather. Devices like Amazon's Alexa can now integrate via IoT to numerous other household items, including lighting, home appliances, and home security systems.

The major players in the voice assistant space that we will be discussing in this paper are Amazon's Alexa, Google Assistant, and Apple's Siri, all of which are capable of interacting with other devices in the home and collecting data about their users. The current most popular home-based devices are Google's Google Home Assistant and Amazon's Echo Dot, both of which require account setups that store personal unique information about it's owners as well as collect other data about how users interact with the devices and what other devices can be activated via voice commands.

While these devices are obviously extremely popular, practical, and overall add value to consumer's lives, our goal is to bring to light some of the issues around fairness in how voice activated device algorithms are trained, how the devices themselves are priced, as well as privacy concerns in what data these devices store and have access to.

Fairness

For this project, the first aspect our team set out to analyze is the fairness behind the most popular currently implemented voice assistance algorithms in the U.S. To assess how fair these services are, we decided to focus on four main aspects of this industry: pricing, user base, device accuracy, and quality of the results. These four are closely interrelated, as how products are priced tend to define what the user base will look like, and in this case, this would then determine what kind of data is collected for training and improving the models. Thus, we believe that these four factors have the potential to create bias in this branch of machine learning and the "smart" devices industry.

Our definition of fairness is stated as the "delivery of equivalent results and benefits to users of smart assistants regardless of their race, gender or socioeconomic status".

Accessibility through Pricing

Stemming from this definition we can first do a quick analysis on the fairness behind these smart assistant enabled devices. Being available in almost all smartphones today, it would be fair to assume that, as of February 2021, at least 85% of the United States' population has

access to a smart assistant[1]. Given that the demographics of smartphone owners are apparently unbiased, one could assume that pricing is not a contributing factor to the potential bias within this industry. However, when we include other devices, specifically smart speakers, is when we see how bias can be introduced. Although 1 out of every 4 adults in the U.S. reportedly own a smart speaker, surveys have shown that this ownership is distributed unequally, as people in households earning more than $75,000 a year are twice as likely to have one of these devices at home than those in households earning less than $30,000 a year[2].

Voice Recognition

With this in mind, one can speculate that there are certain societal groups who are overrepresented in the data gathered from these devices, which in turn trains the algorithms used by these products to better serve them, instead of people who might not be able to afford a smart speaker.

Considering that white families tend to have more wealth on average than families of other races[3], this gives us the intuition that the information gathered by smart speakers, which is then used to train the algorithms that power these smart assistants, will be biased towards Caucasians in an upper socio-economic status. This is problematic, and unfair according to the definition above, as these smart assistants have become better at serving people with specific accents, something that historically is closely related to race and a person's upbringing.

There have been multiple studies that outline this difference in accuracy of smart assistants when recognizing speech from people of different demographics, particularly people of different races. These studies have found that smart assistants tend to understand speech from white people 81% of the time, while only understanding speech from black people 65% of the time[4]. A Stanford study in 2020 found that, across the major devices in the space, the error rates in speech recognition are higher across the board for black people than white people. Additionally, individuals with a heavier dialect (higher dialect density measure or DDM), which tend to be black individuals, have higher WER (word error rates) on average.[5]

---

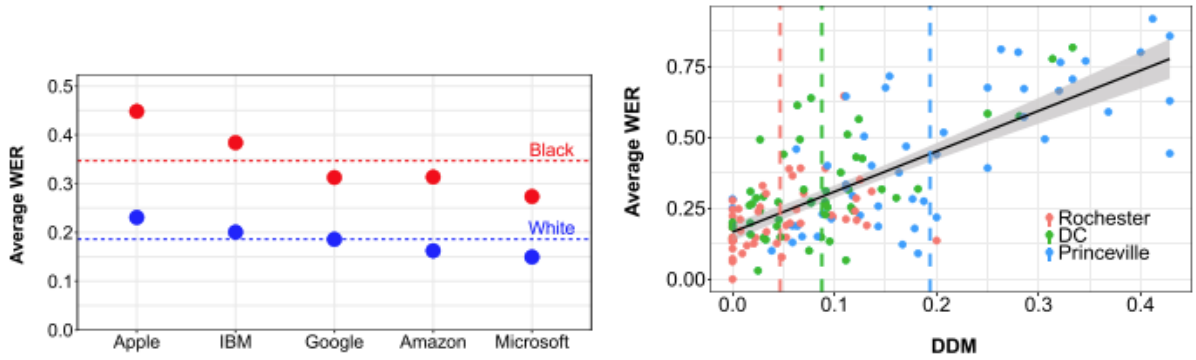
[1] https://www.pewresearch.org/internet/fact-sheet/mobile/

[2]https://www.pewresearch.org/fact-tank/2019/11/21/5-things-to-know-about-americans-and-their-smart-speakers/

[3]https://www.federalreserve.gov/econres/notes/feds-notes/disparities-in-wealth-by-race-and-ethnicity-in-the-2019-survey-of-consumer-finances-20200928.htm

[4]https://www.theverge.com/2020/3/24/21192333/speech-recognition-amazon-microsoft-google-ibm-apple-siri-alexa-cortana-voice-assistant

[5] https://www.pnas.org/content/117/14/7684



These results lead us to believe that the algorithms used by these assistants are biased against non-white users, and thus are not fair. However, it is important to note that the biggest players in this industry are aware of these issues and are working on solving them. We believe that as this technology becomes more available to more people, it could be transformed into a fair product for all users.

Quality of Results and Level of Functionality

In theory, when controlling for the quality of the speech recognition, the quality of the results in voice assistants should be the same. A black person asking about the weather would not get a different result than white person, so by our definition, it would be fair.

On the other hand, the extent of a voice assistant's functionality can be highly dependent on the network of smart devices in a home. An individual with a home full of smart light bulbs would be able to benefit from the voice assistant to a higher degree than an individual with a 'traditional' home. The benefits gained from a voice assistant would be different in this scenario, depending on an individual's level of connectivity. In a study around digital inequalities in the IoT space (which includes smart speakers and smart home systems), researchers found that people with "higher incomes are more likely to use the IoT, which enables them to subsequently develop IoT skills, thus resulting in a greater diversity of IoT use."[6]

This could also further propagate the inequality in voice recognition, whereby individuals who experience more functionality would use the voice assistant more often, thus having more data points to improve the voice recognition algorithm based on the voices of those who can afford smart systems.

[6]Alexander J. A. M. van Deursen, Alex van der Zeeuw, Pia de Boer, Giedo Jansen & Thomas van Rompay (2021) Digital inequalities in the Internet of Things: differences in attitudes, material access, skills, and usage, Information, Communication & Society, 24:2, 258-276, DOI: 10.1080/1369118X.2019.1646777

Ethical Frameworks on Fairness in Voice Assistants

Based on our definition around fairness, we conclude that voice assistants are technically unfair. With that said, there are different viewpoints on whether or not this unfairness should limit the use of voice assistants.

Deontologist	*Nobody should have access to this kind of technology since it is unfair*
Consequentialist	*Because the benefits outweigh the harm, voice assistants should be used regardless of fairness.*
Virtue Ethicist	*Because the intentions for voice assistants are good, fairness is irrelevant.*

Privacy

What data is stored?

Voice assisted smart devices are capable of collecting three different data types about its users. Everything from a grocery list to an intimate conversation in your home is capable of being recorded by voice assistants. With growing concerns over the last few years regarding data hacking and private data leaks, these newer devices can pose new privacy risks to consumers. Below are the three main types of data smart voice assistants can collect.

1. Just like many other smart personal and home devices, general personal information is tied to your voice assistant account (i.e. Google, Amazon, Apple accounts) such as your name, address, or even credit card number. Additionally, some devices like Amazon's, are tied to your Amazon account which stores your purchase and subscription information. This kind of data is largely already stored by companies like Google, Amazon, and Apple regardless of any voice assistant tool.

2. Voice assistants take recordings of your voice when you speak to it and save those recordings to train the built-in speech recognition AI. This Artificial Intelligence is essentially a complex Natural Language Processing model that is trained to recognize the voices of frequent users. Some Amazon devices require advanced voice recognition and a security PIN to set up voice activated purchasing.

   While individual voice recognition may seem concerning, it's actually designed to improve the functionality of the assistant (i.e. eliminating the need to repeat yourself if the device does not understand you the first time). Additionally, Amazon and Google devices are able to distinguish guest voices from resident voices, however, neither are

able to restrict which commands guests can give as opposed to actual users, which can pose other risks.

3. Lastly, the third type of data collected by smart devices are habitual or pattern based data. For example, a device may recognize your command to “listen to the weather” every morning between 8 and 9 AM, and record that as a pattern that a user exhibits.[7] Other patterns a smart device may collect are how many other smart devices are in the network in your house. If you use a smart security system for your home, your devices may have a record for the number of doors in the house, or which areas have cameras.

Ethical Frameworks on Privacy Issues

The more private data these voice assistants like Echo or Google Home collect and store, the better their services will be. The data can be as private as personal accents and family conversations. You have to relinquish the private control of your voice and data by utilizing the devices. Other than just voice recordings, people connect other apps related to financial safety and physical smart home devices to smart assistants. For example, people connect voice assistants to robot vacuum cleaners that go around the home which lead access to the layout of homes.

From a consequentialism point of view, the benefit of the majority of people getting much more convenient assistants at home seems to outweigh the privacy data ownership concern. Although the usage of voice assistants is now limited to very simple tasks, this technology has a lot more room to grow in the future, but only if people are using it increasingly. Even though there exists a risk of data leakage, the cost of privacy seems little compared to the potential convenience that voice assistants are expected to bring to our lives like any revolutionary invention of the past.

However, from a deontological point of view, the act of taking a lot of people’s private data to make money and expose them under unknown risk is not ethical. For example, people can hack into voice assistants to control door locks easily if they want to. No matter whether voice assistants’ usage will be super powerful as the technology develops or not, the pure act that giant companies know about this problem and still continuing selling those products is deemed unethical in deontology.

Risk of Safety on Voice Assistants

People from the University of Michigan have found a way to command smart home devices by hacking into voice assistants remotely with a laser beam without making any sound. The microphones on the smartphones or ipads which control smart lights, ACs, door locks and garages can be hacked as far as a football field with $1000 dollars value equipment by a smart

[7] https://www.blog.google/perspectives/scott-huffman/five-insights-voice-technology/

high school kid from a technical perspective. About 320 million smart speakers are installed 2021 worldwide now and most people are exposed to this risk without knowing.

Although all big brands of voice assistants claim that they differentiate customers from each others' voices, it doesn't solve the problem of one-to-one accuracy of commands. People can still use similar voices to command virtual assistants to do unethical things. Also, there are so many deepfake softwares of voices that people can use. So, it doesn't even matter if the voice assistants can distinguish your own voice for safety.

People can be tracked individually with just some sparse data. With more and more voice assistants people use, the sparse data will exponentially increase in audio files rather than just mostly texts in the past. This will expose people to much more risks if data storage safety technology is not improving along the way.

Terms of privacy and data retention

Virtual assistants have grown in number and popularity. As expected, this growth comes with some security and privacy challenges. As discussed in class, companies can online track you for multiple reasons especially for marketing and improving their services. They can collect their data from each one of the interactions and could even share it with third party companies. Therefore, we decided to search the terms of privacy and data retention for the top 3 virtual assistants in the market. Our goal is to explore if the companies are clear and precise about the data they collect through the audio recording. Specifically, what do they do with it and how long it stays stored in their servers. We explore that in the following table:

Amazon - Alexa[8]	**Google Assistant**[9]	**Apple - Siri**[10]
➔ Amazon processes and retains your Alexa Interactions, such as your voice inputs, music playlists, your Alexa to-do and shopping lists, in the cloud to provide, personalize and improve the services. ➔ No audio is stored or sent to the cloud unless the device detects the wake word (or pressing the Alexa button) ➔ You can delete voice recordings one by one, by date range, by Alexa-enabled device or all at once. ➔ There is an option to not save any voice recording or automatically delete them in a period of time. ➔ If you choose not to have any voice recordings saved, Amazon retains the text transcripts for 30 days ➔ You can configure voice purchasing. You can require a confirmation code, turn purchasing off, etc. ➔ Amazon could keep records of the requests even after the voice recording is deleted (transcripts, actions Alexa took, etc.) Third parties – any Alexa skill, service, application provided by a third party ➔ Amazon shares relevant information with third parties such as your Zip Code for weather app, music playlist for music applications, etc. Amazon keeps voice recordings until the customer decides to delete them.	➔ Google assistant is designed to wait in stand by model until it is activated (Wake word: “Hey Google”) ➔ If you use voice assistant to make a call, it collects call and message log information like your phone number, calling-party numbers, receiving-party number, forwarding numbers, sender, and recipient email address, time and date of calls and messages, duration of calls, routing information and types and volumes of calls and messages. ➔ It collects sensor data (ambient light measurements, temperature, humidity, carbon monoxide and smoke levels) ➔ Audio and video data from devices with cameras and microphones and information derived from this data (coughing, snoring, facial recognition, activity detection, etc.). ➔ Data can stop being visible to you but stay in Google backup systems. The company encrypts to make sure the data is unreadable and inaccessible.	➔ Personal information will not be shared with third parties for their own marketing purposes. However, Apple may use, transfer and disclose non-personal information for any purpose ➔ Apple stores transcripts of your interactions with Siri and Dictation and may review a subset of these transcripts. ➔ The user can opt in to have the audio interactions stored and reviewed by Apple ➔ Stores data for six months where it dissociates from the audio recording random identifier ➔ After six months, it could be retained for up to two years for ongoing improvement of Siri.

[8] Alexa Terms of Use: t.ly/SydI
[9] Google Privacy Policy: https://policies.google.com/privacy#inforetaining
[10] Ask Siri, Dictation and Privacy - https://support.apple.com/en-us/HT210657

The terms of privacy were accessible on each company website. Amazon and Google had multiple and long privacy policies that sometimes could be exhausting and repetitive. However, Apple terms of privacy were shorter, open and direct.

The most important finding was the data retention policy for each company. Even when the user deletes the voice recordings, the three companies retain transcripts for a period of time, or indefinitely. Apple is the only company that openly mentions the data period retention which could be up to two years. Google mentioned in their terms of privacy that they keep the records encrypted even after the user deletes them. As discussed in class, keeping “Anonymized”/ “de-identified” data still can identify users with any other public information. Therefore, if there is a privacy leak it could be possible the hacker could identify the users even after they decided to delete their recording. Moreover, keeping the voice audios or transcripts means having sparse data and a combination of these records could uniquely identify a user.

Another interesting point is that the privacy for third person could be affected (Network Privacy). For example, for Google Assistant, if the user decides to call a person using the voice assistant, it stores the call information from the sender and receiver. By doing this, Google now has information about this third person affecting his/her privacy too.

The reality of virtual assistants is that you’re essentially allowing them into your home at all times. Is the privacy trade-off worth it? This could answer with two possible points of view:

Loss of privacy is an inevitable consequence of technological progress

As technology keeps growing, we need to be aware that we are going to continue losing privacy. Virtual Assistants have many advantages such as helping you keep your home safe, save money in bills and make your life easier. We just can’t stop benefiting from new technologies because we are worried about privacy issues. Companies need the data to keep improving their technologies and eventually improving our day by day.

Balance between performance and privacy

Yes, technology is important and is part of our day by day, but we should still have the right to our privacy. Data retention policies should be created, and companies should comply with them. These regulations should be fair with both sides and allow companies to improve their services while ensuring our privacy.

Sources

- https://www.pnas.org/content/117/14/7684
- https://www.theverge.com/2020/3/24/21192333/speech-recognition-amazon-microsoft-google-ibm-apple-siri-alexa-cortana-voice-assistant
- https://www.tandfonline.com/doi/full/10.1080/1369118X.2019.1646777
- https://www.pewresearch.org/internet/fact-sheet/mobile/
- https://www.statista.com/statistics/1171363/share-of-voice-assistant-users-in-the-us-by-device/
- https://www.pewresearch.org/fact-tank/2019/11/21/5-things-to-know-about-americans-and-their-smart-speakers/
- https://www.federalreserve.gov/econres/notes/feds-notes/disparities-in-wealth-by-race-and-ethnicity-in-the-2019-survey-of-consumer-finances-20200928.htm
- https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740#:~:text=You%20control%20Alexa%20with%20your,personalize%2C%20and%20improve%20our%20services.
- https://policies.google.com/privacy#inforetaining
- https://support.apple.com/en-us/HT210657
- https://www.youtube.com/watch?v=ozIKwGt38LQ

Outline / Contributions

Introduction (Jordan)
- Use of voice assistants.
- Diversity of voice assistants.
- Current state of voice assistants.
- Paper goal

Fairness: General to all voice assistants
- Pricing: Limiting to certain demographics? (Antonio)
- Users: Is the user base biased towards a certain demographic? (Antonio)
- Accuracy in Voice Recognition (Antonio / Christian)
- Quality of results and functionality (Christian)
- Conclusion / Ethical viewpoints of fairness (Christian)

Privacy
- How and what data is stored (Jordan)
- Consequentialist v. Deontological (Trading privacy with quality?) (Sylar)
- Safety of smart home devices getting hacked (Sylar)
- What happens with the voice recordings? Do they sell that info? (Mara)
- Terms of privacy with third parties for those three companies. (Mara)
- Privacy section wrap up (Mara)

Sources